Data Breach Policy

1. Purpose

The purpose of this policy is to ensure that a standardized approach is implemented in the event of a personal data breach. This policy provides general principles and an approach model to respond to and mitigate breaches of personal data.

The policy lays out the actions for successfully managing the response to a data breach as well as comply with the regulation and should be read in conjunction with the *Privacy Policy*.

2. Application

The policy and procedure apply to:

- all personal data created or received by UniSmarter in any format (including paper), whether used, stored on portable devices and media, transported from the company physically or electronically or accessed remotely;
- personal data held on all IT systems.

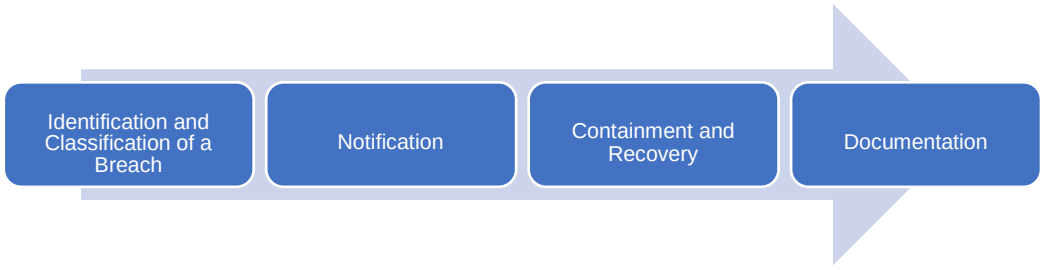
3. Personal Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, modification, unauthorized disclosure or use of, or access to, personal data. This includes breaches that are the result of either accidental or deliberate causes. It also means that a breach is more than just about losing personal data.

4. Data Breach Process and Management

It is the policy of the company that in the event of an information / data breach occurring, the subsequent breach management plan is stringently adhered to. There are key components to the breach management plan, namely:

- Identification and Classification;
- Notification of Breach;
- Containment and Recover;
- Evaluation and Response.



UniSmarter has a Breach Response Team (BRT) which will be responsible for managing any breach of data. The team will include:

- General Manager (in the absence of whom, Head of Academic Operations);
- Academic Director;
- Head of IT.

5. Notification of a Data Breach

When a personal data breach has occurred, UniSmarter needs to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then UniSmarter must notify the relevant regulatory authorities as mandated by law.

5.1 Notification to Data Subjects

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, UniSmarter will inform those individuals without undue delay. In other words, this should take place as soon as possible. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

The following information needs to be included in the notification of data breach to the Data Subjects, in clear and plain language:

- the nature of the personal data breach;
- the name and contact details of the relevant UniSmarter contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken, or proposed to be taken, to address the data breach, including those being taken to mitigate any possible adverse effects.

A *Notification to Data Subject* is not required if:

- personal data is rendered unintelligible to any person who is not authorized to access it, such as through encryption;
- subsequent measures taken ensures that serious harm or high risk to the rights and freedoms of the data subject / s is no longer likely to materialize; or
- it would involve disproportionate effort to individually communicate with each of the data subjects. In such a case, there shall instead be a public communication whereby the data subjects are informed in an equally effective manner.

6. Containment and Recovery

Containment comprises restricting both the scope and impact of the breach. If a breach occurs, the following steps will be undertaken:

- the BRT will decide who will take the lead in investigating the breach and ensure that the appropriate resources are available to the nominated officer for investigation;
- the nominated officer will then establish whether there is anything that can be done to recoup losses and / limit the damage the breach may cause;
- details of the facts relating to the breach, its effects and remedial action taken are then entered in the Data Breach Register.

6.1 Risk Assessment

In assessing the risk arising from the breach, the BRT will consider the potential adverse consequences for individuals, including:

- the nature of the information / data involved;
- the sensitivity of the information / data involved;
- any security mechanisms in place (eg encryption);
- what the information / data could convey to a third party about the individual;
- how many individuals are affected by the breach; and
- whether there are wider consequences / implications to data security.

7. Evaluation and Response

Subsequent to any information / data security breach, a thorough review of the event will be undertaken by the management who will consider:

- what action needs to be taken to reduce the risk of future breaches and minimize their impact;
- whether policies, procedures or reporting lines need to be amended to increase the effectiveness of the response to the breach;
- whether weak points in security controls exist that need to be strengthened;
- whether all students and staff members are cognizant of their responsibilities for information security and adequately trained;
- whether additional investment is required to lessen exposure and if so, the associated resource implications;
- whether any changes to policies and / or procedures are required, with any revisions documented and implemented as soon as possible.

8. Data Breach Record Keeping

UniSmarter needs to record all breaches, regardless of whether or not they need to be reported to the regulatory authorities.

Amendment History

Department:	Academic Affairs
Approval Authority:	
Initial Approval Date:	7th July 2020
Date for Next review:	

Revision Date	Version	Summary of changes
07/07/2020	1	Original